УГОЛОВНО-ПРАВОВЫЕ НАУКИ
CRIMINAL LAW SCIENCES

CC BY

Оригинальное теоретическое исследование

УДК 343.3

https://doi.org/10.23947/2949-1843-2026-4-2-80-88

EDN: QRGVRC

Правовая сущность кибертерроризма и его соотношение со смежными составами преступлений в уголовном праве России

И.Г. Сагирян[1] ✉, **С.И. Кузина**[1, 2]

[1] Донской государственный технический университет, г. Ростов-на-Дону, Российская Федерация

[2] Южно-Российский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте РФ, г. Ростов-на-Дону, Российская Федерация

✉ sagiryan@yandex.ru

Аннотация

Введение. В последние годы кибертерроризм стал одним из основных вызовов национальной безопасности Российской Федерации, поскольку позволяет без особых усилий и финансовых затрат продвигать террористическую идеологию, осуществлять подготовку террористических атак, вести вербовку – одним словом, совершать преступления террористической направленности в киберпространстве без страха быть обнаруженными. На фоне ускоряющихся темпов информатизации, интернационализации информационных сетей и роста оборотов цифровой экономики вопросы обеспечения кибербезопасности приобрели особую актуальность**.** Целью исследования является изучение правовой сущности кибертерроризма как специфической формы террористической деятельности и выявление его соотношения со смежными составами преступлений в уголовном праве РФ.

Материалы и методы. Исследование выполнено на базе норм действующего уголовного права России, отчетов МВД РФ, судебной практики, научных публикаций. Применен диалектический метод познания как основной, а также использованы сопоставительный, формально-юридический, системный подход, общенаучные методы анализа, синтеза, индукции.

Результаты исследования. Проанализировано правовое регулирование террористических преступлений, совершаемых в киберпространстве. Кибертерроризм рассмотрен с позиции объективного следствия глобализации информационных процессов и появления компьютерных сетей. Обосновано положение о том, что кибертерроризм представляет угрозу национальной безопасности РФ, о чем свидетельствует стремительный рост террористических преступлений с использованием информационных технологий, наносящих значительный вред критически важной инфраструктуре государства.

Обсуждение и заключение. Проведенное исследование дополняет и расширяет научное представление о сущности кибертерроризма как потенциальной угрозы национальной безопасности Российской Федерации. Полученные выводы могут послужить основой для дальнейших научных изысканий в данной области.

Ключевые слова: кибертерроризм, национальная безопасность Российской Федерации, уголовное право, угроза, террористический акт, информационно-коммуникационные технологии

Благодарности. Авторы выражают благодарность рецензентам, чья критическая оценка материалов и предложения по их совершенствованию способствовали повышению качества статьи.

Для цитирования. Сагирян И.Г., Кузина С.И. Правовая сущность кибертерроризма и его соотношение со смежными составами преступлений в уголовном праве России. *Правовой порядок и правовые ценности.* 2026;4(2):80–88. https://doi.org/10.23947/2949-1843-2026-4-2-80-88

© Сагирян И.Г., Кузина С.И., 2026

Original Theoretical Research

The Legal Nature of Cyberterrorism and Its Relationship with the Corpora Delicti of Overlapping Offences in the Criminal Law of the Russian Federation

Inga G. Sagiryan[1] ✉, **Svetlana I. Kuzina**[1, 2]

[1] Don State Technical University, Rostov-on-Don, Russian Federation

[2] South-Russian Institute of Management – Branch of the Russian Presidential Academy of National Economy and Public Administration (RANEPA), Rostov-on-Don, Russian Federation

✉ sagiryan@yandex.ru

Abstract

Introduction. In recent years, cyberterrorism has become one of the main challenges to the national security of the Russian Federation, as it allows promotion of terrorist ideology, preparation of terrorist attacks, and recruitment of terrorists without much effort and financial investment, i.e. makes it possible to commit terrorist crimes in cyberspace without fear to be discovered. Amid the backdrop of computerization rate acceleration, internationalization of information networks, and digital economy turnover growth, the problem of ensuring cybersecurity has become particularly relevant. The aim of the present study is to investigate the legal nature of cyberterrorism as a specific form of terrorist activity and to identify its relationship with the corpora delicti of overlapping offences in the criminal law of the Russian Federation.

Materials and Methods. The study was conducted based on the acting norms of the criminal law of the Russian Federation, reports of the Russian Ministry of Internal Affairs, data on the judicial cases, and scientific publications. The dialectical method of cognition was used as the primary one, and was supplemented by the comparative, dogmatic, and system analysis methods, as well as by the general scientific methods of analysis, synthesis, and induction.

Results. Legal regulation of terrorist crimes committed in cyberspace has been analysed. Cyberterrorism was studied from perspective of it being an objective consequence of the processes of information globalisation and emergence of computer networks. The statement about cyberterrorism posing a threat to the national security of the Russian Federation has been substantiated, which is confirmed by the rapid growth of the terrorist crimes committed using the information technology and significant damage caused by them to the critical infrastructure of the state.

Discussion and Conclusion. The conducted research supplements and expands the scientific understanding of the nature of cyberterrorism as a potential threat to the national security of the Russian Federation. The findings obtained may serve a basis for further scientific research in this field.

Keywords: cyberterrorism, national security of the Russian Federation, criminal law, threat, terrorist act, information and communication technologies

Acknowledgements. The authors are grateful to the reviewers for critical evaluation of the materials and suggestions for their improvement that contributed to the significant enhancement of the quality of the article.

For Citation. Sagiryan IG, Kuzina SI. The Legal Nature of Cyberterrorism and Its Relationship with the Corpora Delicti of Overlapping Offences in the Criminal Law of the Russian Federation. *Legal Order and Legal Values*. 2026;4(2):80–88. https://doi.org/10.23947/2949-1843-2026-4-2-80-88

Введение. Современная эволюция технологий изменила не только социально-экономическую жизнь общества, но и структуру преступности. Одним из наиболее опасных проявлений цифровой эпохи становится кибертерроризм. Это специфическая форма террористической активности, реализуемая посредством информационно-коммуникационных технологий и цифровой инфраструктуры и направленная на причинение существенного вреда общественной безопасности, запугивание населения. В доктринальном смысле кибертерроризм представляет собой сложный феномен, находящийся на пересечении уголовно-правовых запретов, норм о противодействии терроризму, положений об охране критической информационной инфраструктуры.

В действующем законодательстве Российской Федерации нормативное закрепление кибертерроризма отсутствует. Между тем в современном понимании кибертерроризм может выражаться в целенаправленном вмешательстве в работу информационных систем, нарушении функционирования государственных информационных ресурсов, атаке на экономические объекты, распространении угроз, дезинформации, а также в иных формах воздействия, способных повлечь за собой дестабилизацию социальной обстановки. По данным отчета МВД РФ за 2024 г., доля преступлений, совершенных с применением информационно-коммуникационных технологий и квалифицированных как террористические, выросла на 20 % по сравнению с 2023 г. Статистика 2025 г. обнаде-

живает: «Число киберпреступлений снизилось на 10,8 % в России за 11 месяцев 2025 г. по сравнению с аналогичным периодом прошлого года», – сообщается на сайте МВД Медиа[1]. Между тем спектр угроз существенно не изменился: атаки на энергообъекты, транспортные системы, банковскую инфраструктуру продолжаются.

Целью исследования является изучение правовой сущности, ключевых признаков кибертерроризма как специфической формы террористической деятельности в цифровой среде, а также выявление его соотношения со смежными составами преступлений, такими как террористический акт, неправомерное воздействие на критическую информационную инфраструктуру РФ, преступления в сфере компьютерной информации.

Материалы и методы. Исследование выполнено на базе норм действующего Уголовного кодекса РФ (ст. 205 (террористический акт), ст. 274.1 (неправомерное воздействие на критическую информационную инфраструктуру РФ), гл. 28 ст. 272–274 (преступления в сфере компьютерной информации)), ежегодных отчетов МВД РФ, судебной практики, научных публикаций.

В исследовании был использован диалектический метод, позволивший рассмотреть динамику кибертерроризма как деструктивного явления, который развивается и изменяется во времени. Сопоставительный метод познания позволил выявить сходства и различия в правовом регулировании кибертерроризма на национальном и международном уровнях. Применение формально-юридического метода способствовало анализу норм УК РФ, судебной практики и доктрины для выявления сущности и разграничения состава преступлений. Через буквальное и системное толкование были разобраны диспозиции статей УК РФ, а также понятие «кибертерроризм». Системный подход интегрировал кибертерроризм в структуру уголовного права как целостную систему. Были рассмотрены взаимосвязи со смежными институтами. Методы анализа, синтеза и индукции позволили объединить разрозненные данные в концептуальную модель кибертерроризма как гибридного преступления с элементами терроризма и киберпреступлений и обобщить полученные результаты. Комплексное использование этих методов обеспечило теоретическое раскрытие сущности кибертерроризма и практическую ценность исследования для совершенствования отечественного законодательства.

Результаты исследования. В Российской Федерации ежедневно около 100 млн человек пользуются информационной сетью Интернет, что свидетельствует о масштабности ее влияния на повседневную жизнь граждан. Несомненно, цифровые технологии приносят значительные преимущества как в сфере государственного управления, так и в предпринимательской деятельности, однако наряду с этим глобальный характер сети Интернет создает почву для возникновения различных угроз. Особую обеспокоенность со стороны государства, правоохранительных органов и общества в целом вызывают преступления, совершаемые в киберпространстве, для которых такие категории, как анонимность и трансграничность сети Интернет создают условия для противоправной деятельности. Некоторые преступления террористической направленности по значимости сопоставимы с посягательствами на национальную безопасность российского государства, так как последствия успешных кибератак на критически важные инфраструктуры могут быть фатальны: от блокировки государственных сервисов до подрыва экономической и социальной стабильности.

Так, 28 июля 2025 г. произошла хакерская атака на российскую компанию «Аэрофлот». Хакерские группировки Silent Crow и Киберпартизаны BY заявили об уничтожении IT-системы авиаперевозчика «Аэрофлот»[2]. Они находились во внутренней сети на протяжении года. Компания полностью лишилась инфраструктуры: не работали кассы, сайт, внутренние сервисы и компьютеры. Авиасообщение фактически было остановлено, отменено более 100 рейсов. Все процессы жизнеобеспечения компании оказались парализованными. Восстановление систем «Аэрофлота» после хакерской атаки заняло больше полугода, а для полной стабилизации потребовался год. Финансовый ущерб составил более 50 млн долларов.

Заметный рост киберпреступлений в 2024 г. и незначительный спад в 2025 г. места для оптимизма не оставляют – это не просто статистика, а серьезная и угрожающая тенденция. Киберпреступления мутируют с такой скоростью, что наши правоохранительные органы, к сожалению, заметно отстают в плане применения новых поисковых систем и информационных технологий, что затрудняет процесс противодействия этому виду преступлений. По информации «Лаборатории Касперского», к киберпреступлениям относят около 12 основных разновидностей – при этом кибертерроризм как вид информационного преступления «Лаборатория Касперского» в расчет не принимает. К сожалению, в настоящее время в отношении данного вида преступлений не выработан четкий понятийный аппарат и, соответственно, меры по противодействию ему.

[1] *МВД рассказало о снижении числа киберпреступлений в России.* URL: https://ria.ru/20251224/chislo-2064367213.html?ysclid=mo44txmo8u802707404 (дата обращения: 18.04.2026).

[2] *Хакеры Silent Crow заявили, что уничтожили IT-систему «Аэрофлота».* URL: https://www.sovsekretno.ru/news/khakery-silent-crow-zayavili-chto-unichtozhili-it-sistemu-aeroflota/ (дата обращения: 18.04.2026).

Вместе с тем для кибертерроризма, как и для терроризма в классическом понимании, характерны публичность, дестабилизация государственных институтов, воздействие на принятие решений, причинение ущерба объектам жизненно важной инфраструктуры. В отличие от обычного терроризма, кибертерроризм преследует два основных типа целей – «пропаганда движения и его идеологии, давление на государственную власть и получение морального удовлетворения от потенциального успеха» [1, с. 134]. Для достижения своих целей кибертеррористы используют технические и цифровые средства при совершении кибератак. Эти атаки подразделяются на две категории: вирусные и информационные. Вирусные атаки включают в себя различные типы вредоносного программного обеспечения:

– бэкдор-вирусы (backdoor-virus): используют программные уязвимости системы, позволяя получить удаленный доступ к устройству;

– полиморфные вирусы: это «многоликие» вирусы, которые постоянно изменяют свой код, затрудняя обнаружение и противодействие антивирусными программами;

– бут-вирусы: атакуют компьютер в момент загрузки системы, что может привести к полному удалению всех данных и самой операционной системы.

Наибольшую опасность представляют целевые продолжительные атаки (advanced persistent threat, APT), способные вывести из строя целые государственные системы, реестры и пр. Это наиболее опасные и технически сложные атаки. Они часто используют уязвимости «нулевого дня» (ранее неизвестные уязвимости) для получения доступа к сети и ресурсам компании. Примером такой масштабной кибератаки является кибертеракт, который произошел 7 октября 2024 г. и привел к массовому сбою в работе электронной судебной системы Российской Федерации. Атака затронула множество ключевых компонентов судебной системы и интернет-портал ГАС «Правосудие». Отметим, что ответственность за этот кибертеракт взяла на себя проукраинская хакерская группировка BO Team, которая ранее уже заявляла о своей причастности к взлому государственной телерадиовещательной компании ВГТРК и отечественного видео-хостинга RuTube.

Что касается нормативно-правового регулирования ответственности за кибертерроризм, то отечественный законодатель до сих пор не установил унифицированной дефиниции. К сожалению, кибертерроризм как явление, посягающее на систему государственного управления, находится, на наш взгляд, в правовом вакууме. По мнению профессора А.В. Серебренниковой, «обсуждение кибертерроризма в большинстве проводится в средствах массовой информации с присущей для журналистов склонности к приукрашиванию и драматизации, а не к научной точности и лаконичности в определении новых терминов» [2, с. 48].

Среди многочисленных вариантов, предлагаемых российскими учеными-правоведами, наиболее удачным, по нашему мнению, является определение В.А. Васенина: кибертерроризм – это «совокупность противоправных действий, связанных с покушением на жизнь людей, угрозами расправ, деструктивными действиями в отношении материальных объектов, искажением объективной информации или рядом других действий, способствующих нагнетанию страха и напряженности в обществе, с целью получения преимущества при решении политических, экономических или социальных задач» [3, с. 67]. Основное предназначение кибертерроризма заключается в нарушении работы критической инфраструктуры, причинении ущерба или запугивания населения в политических, идеологических или религиозных целях. Другими словами – это умышленные действия, направленные на дестабилизацию и (или) стойкое прекращение деятельности (работы) государственных институтов в информационном пространстве сети Интернет посредством применения вредоносных информационных атак и вредоносного программного обеспечения.

В отечественной научной среде многие ученые полагают, что введение конкретной нормы, устанавливающей ответственность за кибертерроризм, является избыточным и нецелесообразным, потому что уже существует состав преступления, предусмотренный ст. 205 УК РФ (террористический акт). Однако действительность такова, что возникли объективные предпосылки для выделения кибертерроризма в отдельную статью в Уголовном кодексе РФ.

В целом информационная преступность связана с незаконным использованием сведений и информационных технологий, причиняющих ущерб гражданам, организациям или государству. «Это может быть подрыв экономики противостоящего государства, искусственное разжигание политической нестабильности, натравливание внутренней оппозиции в государстве друг на друга и на правящую власть или срывы важных международных договоренностей путем вброса дезинформации» [4, с. 48]. В соответствии с УК РФ основные статьи, регулирующие ответственность за преступления в данной сфере, включают ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных программ», ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации» и др.

Сущность информационной преступности может быть раскрыта сквозь призму глобального характера преступлений, обусловленного транснациональной природой цифровой среды. Не менее значимым признаком выступает относительно низкий уровень субъективного риска для правонарушителя. Третьим существенным признаком является высокая степень латентности, так как значительная часть деяний в информационной среде либо не фиксируется потерпевшими, либо не получает надлежащей правовой оценки.

Особую сложность представляет правильная уголовно-правовая квалификация кибертеррористических деяний, поскольку в практике расследования и судебного рассмотрения возникает необходимость отграничения подобных актов от иных противоправных посягательств. В российском уголовном праве элементы кибертерроризма отражаются в совокупности состава преступлений, предусмотренных ст. 205 УК РФ (террористический акт), а также ст. 272 (неправомерный доступ к компьютерной информации), ст. 273 (создание, использование, распространение вредоносных программ), ст. 274 (нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей).

Соотношение кибертерроризма и традиционного терроризма согласуется со ст. 205 УК РФ, в которой терроризм – совершение взрыва, поджога или иных действий, создающих опасность гибели людей, причинение значительного имущественного ущерба или наступление иных тяжких последствий в целях нарушения общественной безопасности, устрашения населения или воздействия на принятие решений органами власти. Кибертерроризм – это, по сути, одна из новых форм реализации террористической деятельности. Отличительная черта – специфичность инструментов (вместо взрывчатки – вредоносные программы, DDoS-атаки, вмешательство в АСУ ТП). Например, если преступник заражает вирусом систему управления железнодорожным движением, что приводит к массовой аварии, это может быть квалифицировано как террористический акт, совершенный с использованием информационных технологий. Если объектом посягательства выступает общественная безопасность, а деяние элементарно направлено на нагнетание страха, дестабилизацию с использованием кибертехнологий, то речь идет не о киберпреступлении вообще, а именно о кибертерроризме.

Другим распространенным видом преступлений в цифровой среде является хактивизм. «Форма гражданского неповиновения и протеста, когда целью кибератаки является привлечение внимания общественности к социальным, политическим и другим проблемам для достижения социальных или политических изменений, носит название «хактивизм». Хактивизм – форма политического активизма, которая использует технические навыки и технологии, чтобы воздействовать на тех, чьи действия противоречат идеологии хактивистов» [5, с. 342]. Отличительной чертой хактивизма признается провоцирование общества на политические, социальные или иные общественно значимые действия.

Современная действительность породила и такой вид киберугроз, как кибервойны. По определению А.С. Харланова и Р.В. Белого, кибервойны – «это мероприятия по воздействию на поведение людей, подмены их ценностей, изменение истории и сложившихся понятий, толкование различных событий в нужном ключе» [6, с. 107]. Целью кибервойн является нарушение деятельности объектов стратегического значения для причинения вреда национальной безопасности государства, здоровью и жизни людей. А.В. Шидловский утверждает, «по своей природе кибервойна существует в пределах виртуального пространства и сводится к использованию Интернета, а также связанных с ним технических и информационных средств одним государством с целью причинения вреда военной, технологической, экономической, политической, информационной безопасности и суверенитету другого государства» [7, с. 97]. Критическая информационная инфраструктура становится мишенью для посягательства. Основные методы – DDoS-атаки, использование вредоносного ПО, подделка баз данных.

Наконец, непосредственно киберпреступления как обобщенное наименование целого ряда преступлений, целью которых является незаконное обогащение, получение денежного вознаграждения. Их главная отличительная особенность – нацеленность на получение выгоды (денежной или иной), нанесение вреда конкретным субъектам, часто с целью хищения, мошенничества либо паралича отдельных организаций. Жертвами киберпреступников обычно становятся бизнес-структуры и частные лица. Киберпреступники чаще всего используют вредоносные ПО, большей частью программы шифровальщики, фишинг и социальную инженерию. Хакер, внедривший в систему энергокомпании вирус ради вымогательства или шантажа, действует в интересах собственной выгоды – это чаще киберпреступление. Если в деянии отсутствует террористическая цель (устрашение, влияние на власть), то квалификация сводится к статьям о компьютерных преступлениях. Если же мотив преступника – дестабилизация, массовое разрушение, вызов страха – это элемент кибертерроризма. Многие действия, входящие в кибертеррористическую атаку (взлом, распространение вируса, ложная паника), по отдельности – составы преступлений, предусмотренные ст. 272–274 УК РФ, но в совокупности с террористической целью они рассматриваются как квалифицирующий признак, увеличивающий степень общественной опасности деяния.

Кибертерроризм по квалифицирующим признакам схож с диверсией (ст. 281 УК РФ) – совершение взрыва, поджога или иных действий, направленных на уничтожение, повреждение объектов инфраструктуры, транспорта, связи, с целью подрыва экономики и обороноспособности РФ. В контексте кибертерроризма диверсионный акт может быть осуществлен через киберсредства: вредоносная программа, управляющая промышленным оборудованием, саботаж систем связи или транспорта. Саботаж программно-аппаратного комплекса управления локомотивами или электросетями с помощью кибератаки – преступление, внешне схожее с кибертерроризмом, однако основная цель при диверсии – экономический или военно-стратегический урон, а не устрашение населения или давление на власть. Если основная цель – вызвать массовую панику, страх, дестабилизировать общество, – это кибертерроризм. Если же вред критической инфраструктуре – способ воздействия на экономику или обороноспособность без явного элемента устрашения, – то ближе к диверсии.

При прочих различиях объединяющим фактором всех этих видов преступлений остается объект преступного посягательства – компьютерные сети, серверы, мобильные устройства и пр. Квалифицирующим признаком кибертерроризма, отличающим его от иных форм использования информационно-коммуникационных технологий в противоправных целях, является «применение информационно-коммуникационных технологий непосредственно как института совершения деструктивной атаки, а не только средства коммуникации или координации» [8, с. 119].

В сфере цифровой информации совершаются и другие виды преступлений, такие как мошенничество, сетевой шпионаж. Мошенничество представляет собой незаконные действия, направленные на обман ради получения выгоды. В своей преступной деятельности мошенники прибегают к использованию вирусов, троянов и других вредоносных программ. Мошенничество предполагает нарушение систем защиты цифровой информации. Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) – действия, связанные с хищением имущества при помощи информационных технологий. Во всех этих случаях отсутствует террористическая цель, эффект устрашения, влияния на органы власти, массовых последствий для общества. Поэтому такие деяния рассматриваются как самостоятельные составы, не достигающие степени общественно опасного характера, свойственного терроризму. Сетевой шпионаж используется в нарушении законов для получения конкурентного преимущества.

При разграничении кибертерроризма со смежными преступлениями на практике возникает несколько типовых проблем. Мотив преступника может быть неоднозначным (финансовый шантаж с угрозой теракта или чистый террор). Используется комбинированный способ совершения преступления (например, сначала хакерская атака с хищением данных, затем распространение угроз и панических слухов). В международных делах сложно определить юрисдикцию и квалификацию. Особую сложность вызывает доказывание террористической цели и умысла – в таких делах важна тщательная работа следствия, экспертных групп, привлечение специалистов по криминалистике, кибербезопасности.

Кибертерроризм беспрерывно эволюционирует. Компьютерные вирусы, различные атаки на информационные системы, троянские программы, позволяющие выполнять вредоносные действия и заражать системы, известны с начала 2000-х гг. Пользоваться вредоносными программами вначале стали не террористические группировки, а спецслужбы ряда государств, которые находились в состоянии конфронтации с потенциальным противником. Так, в 2007 г. Израиль внедрил троянский вирус в код программного обеспечения сети противовоздушной обороны Сирии. В результате израильские самолеты беспрепятственно проникли на территорию Сирийского государства и нанесли удары по атомной энергетической установке, в то время как на экранах сирийских радаров не было никаких признаков вторжения. Есть и другие примеры: «Вирус Stuxnet представлял собой сложный компьютерный червь, который атаковал иранские ядерные объекты в 2010 г.» [9, с. 27]. Вредоносная программа поражает все на своем пути и в числе первых нанесла вред системе Иранского центра по обогащению урана.

Российская законодательная инициатива старается своевременно реагировать на вызовы современности, однако действительность порождает новые формы киберпреступлений, которые заметно изменяют криминологическую обстановку в стране. Как справедливо отмечает С.С. Витвицкая, «наблюдается такая форма киберпреступления, как кибершпионаж. Существует реальная угроза употребления информационно-телекоммуникационных технологий в ходе внешнеполитических и военных конфликтов для осуществления диверсий на объектах критической информационной инфраструктуры и др. Появились новые формы киберпосягательств на общественную безопасность, здоровье населения, общественную нравственность и другие правоохраняемые объекты» [10, с. 132].

В современных условиях уже невозможно отрицать, что кибертеррористическая опасность затрагивает не отдельное государство, а представляет собой угрозу транснационального характера. Кибератаки не ограничиваются государственными границами и не учитывают ни число пострадавших, ни масштабы причиненного ущерба. Следовательно, добиться ощутимых и устойчивых результатов исключительно силами одного государства в данной сфере невозможно. М.В. Алексеева и Е.А. Филимонова справедливо отмечают, что «действительность диктует условия, при которых ни один аппарат национальной безопасности не имеет возможности самостоятельно

справляться и предусматривает сотрудничество между государствами и грамотно стратегически выстроенную международную политику» [11, с. 51].

В обозримом будущем правоведам предстоит установить признаки и конкретизировать понятие кибертерроризма, с тем чтобы отделить этот вид преступлений от смежных, совершаемых в виртуальном пространстве с использованием информационно-телекоммуникационных технологий. В.Г. Романовский утверждает, что «уголовно-правовая политика современного государства должна эффективно реагировать на складывающиеся обстоятельства, при этом носить упреждающий характер» [12, с. 308]. Необходимо закрепить в Уголовном кодексе РФ специальные виды ответственности за совершение киберпреступлений террористической направленности, а также сформировать систему превентивных мер. При этом, несмотря на сложившуюся современную геополитическую обстановку, в которой находится Россия, наиболее действенным и фактически безальтернативным подходом к противодействию компьютерному терроризму остается международное сотрудничество: взаимодействие правоохранительных органов, обмен информацией между государствами, а также совместная работа специалистов в сфере информационных технологий и экспертов из разных стран.

Обсуждение и заключение. Кибертерроризм – сложное явление, интегрирующее признаки терроризма, экстремизма, компьютерных и иных преступлений, которое создает новые вызовы для национальной и международной безопасности и требует адекватного научного и практического реагирования. Основной квалификационный признак кибертерроризма – наличие цели устрашения, дестабилизации, политического давления, реализуемой с помощью современных информационных технологий.

Резкий рост числа кибератак, направленных именно на объекты критической инфраструктуры, подтверждает, что данные объекты становятся приоритетной целью злоумышленников. Использование зарубежного программного обеспечение и отсутствие криптографической защиты информации ставит под угрозу целостность и работу цифровых государственных сервисов. Поэтому на повестке дня стоит вопрос разработки комплекса мер организационно-технического и правового характера. В первую очередь, это осуществление полного перехода на отечественное программное обеспечение, которое будут обладать криптографической защитой. Это тем более актуально, что наработки в области криптографии, а также нормативно-правовое регулирование в данной области уже имеется. На уровне Судебного департамента при Верховном Суде Российской Федерации необходимо разработать наставление по производству электронных резервных копий материалов дел, произвести балансировку нагрузки серверов судебной системы с запасом, создать резервный сервер (дубликат) ГАС «Правосудие» на случай информационных инцидентов, разработать комплекс контрмер (контратак) на хакерские группировки с целью долгосрочной нейтрализации их деятельности.

Перед правоохранительной и правоприменительной системами России сегодня стоит ряд злободневных задач, требующих незамедлительного решения. Прежде всего, необходимо выработать легальное определение понятия «кибертерроризм». Для назначения адекватной меры ответственности, эффективной защиты общества и государства необходимо также правильное соотнесение кибертеррористического акта и смежных составов. Растущая профессионализация кибертеррористов и использование ими все новых методов воздействия обусловливают необходимость постоянного обновления законодательной базы и внедрения гибких нормативных правовых актов, учитывающих динамику киберугроз.

Самой эффективной мерой борьбы с кибертерроризмом на сегодняшний день является тесное международное сотрудничество, участие в создании международных институтов и инструментов борьбы с кибертерроризмом, прочное взаимодействие правоохранительных органов различных стран. Обмен информацией о киберугрозах, организация совместных оперативно-розыскных действий с привлечением специалистов из IT-сферы являются залогом осуществления превентивных мер по противодействию мировому кибертерроризму. Совершенствование отечественной нормативно-правовой базы, заключение международных соглашений и договоров, направленных на совместное противодействие киберугрозам, имеют первостепенное значение в борьбе с этим мировым злом.

Список литературы / References

1. Цримов А.А. Кибертерроризм как глобальная угроза национальной безопасности. *Пробелы в российском законодательстве*. 2023;16(5):133–137.

Tsrimov AA. Cyberterrorism as a Global Threat to National Security. *Gaps in Russian Legislation*. 2023;16(5):133–137. (In Russ.)

2. Серебренникова А.В. Кибертерроризм: причины и условия. *Colloquium-Journal*. 2021;(17–4(104)):47–49.

Serebrennikova AV. Cyber Terrorism: Causes and Conditions. *Colloquium-Journal*. 2021;(17–4(104)):47–49. (In Russ.)

3. Васенин В.А. Информационная безопасность и компьютерный терроризм. В: *Научные и методологические проблемы информационной безопасности: сборник статей.* Москва; 2004. С. 67–83.

Vasenin V.A. Information Security and Computer Terrorism. In: *Scientific and Methodological Problems of Information Security: Collection of Articles*. Moscow; 2004. P. 67–83. (In Russ.)

4. Мазуров В.А., Стародубцева М.А. Кибертерроризм как оружие в гибридной войне. *Российско-азиатский правовой журнал*. 2020;(1):46–52.

Mazurov VA, Starodubtseva MA. Cyber Terrorism as a Weapon in a Hybrid War. *Russian-Asian Law Journal*. 2020;(1):46–52. (In Russ.)

5. Хижак Н.П. Эволюция хактивизма: новая реальность киберугроз. В: *Труды IX Международной научно-практической конференции «Дистанционные образовательные технологии».* Симферополь: ООО «Издательство Типография «Ариал»; 2024. С. 341–344.

Khyzhak NP. Evolution of Hacktivism: the New Reality of Cyber Threats. In: *Proceedings of the IX International Scientific-Practical Conference "Distance Education Technology".* Simferopol: LLC "Arial" Publ.; 2024. P. 341–344. (In Russ.)

6. Харланов А.С., Белый Р.В. Новые реалии ведения войны: «кибертерроризм» и информационные войны. *Юридическая наука*. 2021;(6):106–110.

Harlanov AS, Beliy RV. New Realities of Warfare: "Cyber Terrorism" and Information Warfare. *Legal Science*. 2021;(6):106–110. (In Russ.)

7. Шидловский А.В. Некоторые аспекты противодействия кибертерроризму и кибердиверсиям. *Право.by* 2017;6(50):96–100.

Shidlovsky AV. Modern Situation and New Approaches to Countering Cyberterrorism and Cybersabotage. *Pravo.by*. 2017;6(50):96–100. (In Russ.)

8. Асрумян А.К. Юридическая природа кибертерроризма: проблемы квалификации и доказательств. *Закон и власть*. 2025;(7):118-122.

Asrumyan AK. The Legal Nature of Cyberterrorism: Problems of Qualification and Evidence. *Law and Power*. 2025;(7):118–122. (In Russ.)

9. Литвинов М.Ю., Алескеров В.И., Баранов В.В., Матвеев Д.А. Противодействие международному кибертерроризму – одно из приоритетных направлений деятельности сотрудников органов внутренних дел Российской Федерации. *Вестник Барнаульского юридического института МВД России.* 2025;(1):25–29.

Litvinov MYu, Aleskerov V.I., Baranov V.V., Matveev D.A. Countering international cyber terrorism is one of the priority areas of activity of employees of the internal affairs bodies of the Russian Federation. *Vestnik Barnaulskogo yuridicheskogo instituta MVD Rossii (Bulletin of the Barnaul Law Institute of the Ministry of Internal Affairs of Russia).* 2025;(1):25–29. (In Russ.)

10. Витвицкая С.С., Витвицкий А.А., Исакова Ю.И. Киберпреступления: понятие, классификация, международное противодействие. *Правовой порядок и правовые ценности*. 2023;1(1):126–136. https://doi.org/10.23947/2949-1843-2023-1-1-126-136

Vitvitskay SS., Vitvitsky AA, Isakova YuI. Cybercrimes: Concept, Classification, International Countering. *Legal Order and Legal Values*. 2023;1(1):126–136. (In Russ.) https://doi.org/10.23947/2949-1843-2023-1- 1-126-136

11. Алексеева М.В., Филимонова Е.А. Актуальные вопросы противодействия угрозам национальной безопасности. *Правовой порядок и правовые ценности.* 2024;2(1):47–53. https://doi.org/10.23947/2949-1843-2024-2-1-47-53

Alekseeva MV, Filimonova EA. Topical Issues of Counteracting the Threats to National Security. *Legal Order and Legal Values*. 2024;2(1):47–53. (Russ.). https://doi.org/10.23947/2949-1843-2024-2-1-47-53

12. Романовский В.Г. Перспективы криминализации кибертерроризма в России и за рубежом. *Академический юридический журнал*. 2022;23(3(89)):302–311.

Romanovskiy VG. Prospects for Criminalization of Cyberterrorism in Russia and Abroad. *Academic Law Journal*. 2022;23(3(89)):302–311. (In Russ.)

Об авторах:

Инга Григорьевна Сагирян, кандидат филологических наук, доцент, доцент кафедры «Уголовное право и публично-правовые дисциплины» Донского государственного технического университета (344003, Российская Федерация, г. Ростов-на-Дону, пл. Гагарина, 1), SPIN-код, ScopusID, ORCID, sagiryan@yandex.ru

Светлана Ивановна Кузина, доктор политических наук, кандидат социологических наук, профессор, профессор кафедры «Уголовное право и публично-правовые дисциплины» Донского государственного технического университета (344003, Российская Федерация, г. Ростов-на-Дону, пл. Гагарина, 1), профессор кафедры политологии и этнополитики Южно-Российского института управления – филиала Российской академии народного хозяйства и государственной службы при Президенте РФ (344002, Российская Федерация, г. Ростов-на-Дону, ул. Пушкинская, 70), SPIN-код, ORCID, svivk@yandex.ru

Заявленный вклад авторов:

И.Г. Сагирян: формирование основной концепции, методология исследования, постановка задач исследования, подготовка текста, формирование выводов.

С.И. Кузина: обзор и анализ научных источников, доработка текста, корректировка выводов.

***Конфликт интересов*: авторы заявляют об отсутствии конфликта интересов.**

Авторы прочитали и одобрили окончательный вариант рукописи.

About the Authors:

Inga G. Sagiryan, Cand.Sci. (Philology), Associate Professor of the Criminal Law and Public Law Disciplines Department, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, Russian Federation), SPIN-code, ScopusID, ORCID, sagiryan@yandex.ru

Svetlana I. Kuzina, Dr.Sci. (Politics), Professor of the Criminal Law and Public Law Disciplines Department, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, Russian Federation), Professor of the Political Science and Ethnopolitics Department, South-Russian Institute of Management of Russian Presidential Academy of National Economy and Public Administration (70, Pushkinskaya St., Rostov-on-Don, 344002, Russian Federation), SPIN-code, ORCID, svivk@yandex.ru

Claimed Contributorship:

IG Sagiryan: formulating the main concept, research methodology, setting the objectives of research, preparing the text, formulating the conclusions.

SI Kuzina: review and analysis of scientific sources, refining the text, correcting the conclusions.

Поступила в редакцию / Received 07.05.2026
Поступила после рецензирования / Reviewed 04.06.2026
Принята к публикации / Accepted 10.06.2026